IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application. An identifier indicating the status of each claim is provided.

Listing of Claims

1-38. (Cancelled)

39. (Currently Amended) An information processing device for supplying management information to a data storage device, said information processing device comprising:

forming means for forming management information that manages a storage area in the data storage device in a layered structure, said storage area divided into a plurality of system blocks and a plurality of user blocks, ~~said management information pertaining to a definition area to be formed in the data storage device, said definition area being used to define storage areas of the data storage device for use in providing services~~;

encrypting means for encrypting said management information, said encrypting means encrypting a lower layer of the management information by using a key contained in an upper layer of the management information;

communication means for communicating the encrypted management information to said data storage device, ~~to enable said definition area to be formed therein based upon said management information~~; and

means for generating a check code to check whether the management information has been tampered with by a non-authorized user,

wherein said encrypting means encrypts the check code together with the management information;

wherein said plurality of user blocks are allocated in an ascending order, said plurality of system blocks are allocated in a descending order, and a boundary between the plurality of user and system blocks is variable; and

wherein said plurality of system blocks are classified into at least three areas, a system defining block area, a defining block area, and a service defining block area.

40. (Previously Presented) The information processing device as claimed in claim 39, wherein said communication means is configured to transmit the encrypted management information through a predetermined transmission medium.

41. (Previously Presented) The information processing device as claimed in claim 39, wherein said forming means forms said management information such that the management information contains a storage area identifying code to be allocated to a storage area of the data storage device to be managed, and is used to identify said storage area.

42. (Previously Presented) The information processing device as claimed in claim 39, wherein said forming means forms said management information such that said management information contains information on the amount of empty capacity of said storage area to be managed.

43. (Cancelled)

44. (Currently Amended) A data storage device comprising:

receiving means for receiving encrypted management information from an external equipment, ~~said management information pertaining to a definition area to be formed in the data storage device, said definition area being used to define storage areas of the data storage device for use in providing services,~~ wherein ~~said storage areas are~~ a storage area is managed with management information in a layer structure and ~~containing~~ contains a key, said storage area divided into a plurality of system blocks and a plurality of user blocks;

decrypting means for decrypting a lower layer of the encrypted management information by using said key, said key being contained in an upper layer of the management information;

data storage means for storing data to supply predetermined services, wherein access to a storage area of said data storage means is provided by said key; and

management information storage means for storing the management information;

~~management means for forming the definition area defining said storage areas in a layered structure, and also managing the storage areas, on the basis of the received management information, and~~

operation means for operating on a cheek code to check whether the management information has been tampered with by a non-authorized user,

wherein said decrypting means decrypts the check code together with the management information;

wherein said plurality of user blocks are allocated in an ascending order, said plurality of system blocks are allocated in a descending order, and a boundary between the plurality of user and system blocks is variable; and

wherein said plurality of system blocks are classified into at least three areas, a system defining block area, a defining block area, and a service defining block area.

45. (Previously Presented) The data storage device as claimed in claim 44, wherein said receiving means provides access to said external equipment through a predetermined transmission medium.

46. (Cancelled)

47. (Previously Presented) The data storage device as claimed in claim 44, wherein said receiving means is arranged to perform the communications with said external equipment in a contact or non-contact state.

48. (Previously Presented) The data storage device as claimed in claim 44, wherein said management information contains a storage area identifying code which can be allocated to said storage area to be managed and is used to identity said storage area.

49. (Previously Presented) The data storage device as claimed in claim 44, wherein said management information contains information on the amount of an empty capacity of said storage area to be managed.

50. (Cancelled)

51. (Currently Amended) An information processing system comprising a data storage device and an information processing device, said information processing device comprising:

forming means for forming management information that manages a storage area in the data storage device in a layered structure, said storage area divided into a plurality of system blocks and a plurality of user blocks;

encrypting means for encrypting said management information, said encrypting means encrypting a lower layer of the management information by using a key contained in an upper layer of the management information; and

communication means for communicating the encrypted management information to said data storage device,

said data storage device comprising:

receiving means for receiving encrypted management information from said information processing device;

decrypting means for decrypting the lower layer of the encrypted management information by using the key contained in the upper layer of the management information;

data storage means for storing data to supply a predetermined service, wherein access to a storage area of said data storage means is provided by said key;

management information storage means for storing said management information; and

~~management means for forming a definition area defining the storage areas of said data storage means in a layer structure, and also managing the storage areas, on the basis of the received management information; and~~

code generating means for generating a check code to check whether the management information has been tampered with by a non-authorized user,

wherein said encrypting means encrypts the check code together with the management information;

wherein said plurality of user blocks are allocated in an ascending order, said plurality of system blocks are allocated in a descending order, and a boundary between the plurality of user and system blocks is variable; and

wherein said plurality of system blocks are classified into at least three areas, a system defining block area, a defining block area, and a service defining block area.

52. (Currently Amended) An information processing method comprising[[,]] the steps of:

forming management information for managing a storage area in a layer structure, said storage area divided into a plurality of system blocks and a plurality of user blocks;

encrypting the management information to provide encrypted management information, with a lower layer of said management information being encrypted by using a key contained in an upper layer of the management information;

communicating said encrypted management information to a data storage device;

decrypting the encrypted lower layer of the management information by using the key;

storing data to supply predetermined services in a storage area of said data storage device, access to the storage area being provided by the key;

storing management information in a management information storage means of said data storage device; and

~~forming a definition area to define data storage areas in a layered structure on the basis of the management information; and~~

generating a check code to check whether the management information has been tampered with by a non-authorized user,

wherein the check code is encrypted together with the management information;

wherein said plurality of user blocks are allocated in an ascending order, said plurality of system blocks are allocated in a descending order, and a boundary between the plurality of user and system blocks is variable; and

wherein said plurality of system blocks are classified into at least three areas, a system defining block area, a defining block area, and a service defining block area.

53. (Cancelled)

54. (Currently Amended) A data storage method for storing data to supply a predetermined service, said data storage method comprising the steps of:

receiving encrypted management information from an external equipment, said management information being provided for managing a storage area in a layer structure and containing a key, said storage area divided into a plurality of system blocks and a plurality of user blocks;

decrypting a lower layer of the encrypted management information by using the key contained in the upper layer of the management information;

storing data to supply a predetermined service in a data storage means, with access to a storage area of said data storage means being provided by the key;

storing management information in a management information storage means;

forming the storage area of said data storage means in a layer structure on the basis

of the management information;

managing the storage area of said data storage means on the basis of the management information; and

operating on a check code to check whether the management information has been tampered with by a non-authorized user,

wherein the check code is encrypted together with the management information;

wherein said plurality of user blocks are allocated in an ascending order, said plurality of system blocks are allocated in a descending order, and a boundary between the plurality of user and system blocks is variable; and

wherein said plurality of system blocks are classified into at least three areas, a system defining block area, a defining block area, and a service defining block area.